RESEARCH ARTICLE OPEN ACCESS

A Study of Security Issues Related With Wireless Fidelity (WI-FI)

Akshika Aneja [1], Garima Sodhi [2]
Assistant professor
Department of Computer Science, GNDU [1]
Department of Computer Science, DAV College [2]
Amritsar – India

ABSTRACT

Wireless technology provides us much profit like portability and flexibility, increased productivity, and lower installation costs. Nowadays, communications through mobiles, computers, laptops, wireless networking technologies have extended to a great level. This does a maximum coverage all over the world. Security issues have also been crossed a level in Wi-Fi network because of the unauthorized users and the Wi-Fi hackers. So to implement the feasible Security WEP, WPA has been proposed in this paper to overcome the feasible security problems. These both protocols are generally used to encrypt the current data and information, so that the unauthorized and hackers cannot be able to decrypt the data and hack the Wireless Fidelity (Wi-Fi) networks. Many accessories can be connected with the Wireless Fidelity network with the help the Access Point (AP).

Keywords:- Wireless Fidelity Technology, Wired Equivalent Privacy (WEP), Wireless Fidelity Protected Access (WPA), Wireless Access Point, *SSID, MAC, WiMAX, DoS*

I. INTRODUCTION

Wireless Fidelity Wi-Fi Technology is one of the upcoming techniques in the internet world. This Wi-Fi can be an alternate to Wired Technology. Wi-Fi is usually used for linking devices in wireless form. Wi-Fi Network attaches computers to one another in a better communicable way. It creates a hidden path between the internet and the wired network. Wi-Fi network functioning can be done on the physical and the data link layer. Radio Frequency (RF) is used for transmitting data through air. This is the very characteristic in the Wi-Fi technology. It also provides enhanced data speeds. IEEE 802.11 is considered as a position of values moving elsewhere can be known as Wireless Local Area Network (WLAN). This is also a type of network communication.

Access Point (AP) is considered as very significant feature in the Wi-Fi network technology. Access Point (AP) has a radio transmitter and also a radio receiver. This directly gets linked with the wired network or to the internet network.

This Access Point (AP) takes a common achievement as a base station for the entire Wi-Fi net-work. Some of the Wi-Fi Network Topologies are given below.

- Access Point AP-based topology
- Star-based network topology
- Peer-to-peer topology
- Point-to-multipoint bridge topology

This Wi-Fi network is facing numerous security problems because of the hackers and also by the unauthorized members. The Wi-Fi hacker uses the Wireless Hacking tools AirSnort, Aircrack, WepAttack, WEPCrack etc above the network.

Wireless Access Point is shown in the Figure 2. It basically helps to connect with devices likes digital cameras, tablet computers and digital audio players, PCs, video-game comforts, smart phones, laptops etc.

II. RELATED WORK

Wireless is in everywhere like

- More devices are using Wi-Fi:- Cell phones
- Digital cameras
- Printers
- PDAs
- Video game controllers
- Televisions
- Speakers
- Refrigerators etc

III. WIRELESS NETWORKS CHALLENGES

Wireless Networks plays the most significant role in the development of the information in among individual-to-individual, business-to-business, and individual-to-business. It changed entirely the way of sharing of the information but still there are lots of challenges which are the hurdles in the wide adaptation of wireless network technology [1], [2].

We have to understand the main harms that not only WI-FI network faces but all the networks faces are – CIA that is confidentiality, integrity and authentication.

Confidentiality:

Allow only the authorized person to examine the encrypted messages or the information.

Integrity:

It is defined as the information not being opened by third person and it should reach in the same format as it was sent by the transfer party.

Authentication:

The parties sending or receiving messages make sure that, who they say they are, and have right to assume such actions.

The main matter in the security of wireless signal is its mode of transmission. Wireless signals are transmitted during the electromagnetic waves; these waves cannot be contained physically. In wireless networks the signals are communicated through air, hence can be easily intercepted with the help of right transceiver equipment.

.IEEE 802.11 Standards:

In 1997, IEEE ratified the 802.11 standard for WLANs. The IEEE 802.11 standard chains three transmission methods, including radio transmission surrounded by the 2.4 GHz band. In 1999, IEEE ratified two amendments to the 802.11 standard—802.11a and 802.11b—that describe radio transmission methods, and WLAN equipment based on IEEE 802.11b quickly became the leading wireless technology [10]. IEEE 802.11b equipment transmits in the 2.4 GHz band, contribution data rates of up to 11 Mbps. IEEE 802.11b was intended to provide performance, throughput, and security features comparable to wired LANs. In 2003, IEEE free the 802.11g amendment, which specifies a radio transmission method that uses the 2.4 GHz band and can carry data rates of up to 54 Mbps. Additionally, IEEE 802.11g-compliant products are backward compatible with IEEE 802.11b-compliant products.[7].

WEP:

WEP protocol is element of the IEEE 802.11 standard [3], [8], [9], [10], [11], [13]. It was introduced in 1997.WEP is used in 802.11 network to defend link level data during the wireless transmission. WEP was the first cryptographic protocol which are developed for the WI-FI to facilitate privacy and authentication. WEP uses the shared key authentication mechanism and is based on secret cryptographic key. WEP protocol uses the RC4 (Rivest Cipher4) stream cipher algorithm to encrypt the wireless communications. This RC4 stream algorithm protects the contents form disclosure to eavesdroppers. WEP support 40-bit key and with addition it also support 128 or even 256 bit key also. WEP was designed to protect a wireless network from eaves dropping. WEP uses linear hash function for data integrity. In WEP there is no key management and no replay detection facility. But in 2001 several serious weaknesses were identified. Now, WEP connection can be cracked within minutes. After having such type of vulnerabilities, in 2003 the WI-FI Alliance WEP had been replaced by WPA. The main trouble of WEP was-it uses static encryption keys.

WPA/WPA2:

WPA and WPA2 are two security protocols developed by WI-FI Alliance [9], [10], [11], [13]. WPA provides developed with the point of solving the problems in WEP cryptographic method. WPA was developed in 2003. Both WPA and WPA2 have two modes of operation: Personal and Enterprise. The Personal mode involves the use of a pre-shared key for authentication, while the Enterprise mode uses IEEE 802.1X and EAP for this point.WPA2 was introduced in September 2004. WPA addresses a subset of the IEEE 802.11i specification that addresses the weaknesses of WEP. WPA2 extends WPA to include the full set of IEEE 802.11i requirements. WPA is easier to configure and it is extra secure than WEP. WPA uses the improved encryption algorithm known as TKIP (Temporal Key Integrated Protocol).TKIP provides each client with a unique key and uses much longer keys that are rotated at a configurable interval. It also includes an encrypted message integrity check field in the packets; this is designed to avoid an attacker from capturing, altering and/or resending data packets which prevent Denial-of-Service and spoofing attack. WPA can be operated with the help of RADIUS server of without RADIUS severs. Now, TKIP can be broken easily. WPA2 uses Advanced Encryption Standard. WPA2 may not work with some older network cards. WPA2 have the 4 main key factors:-

- mutual authentication
- strong encryption
- interoperability
- Ease to use

These are the 4 main advantages of WPA2. WPA and WPA2 use the cryptographic hash function for data integrity. WPA and WPA2 both provides the key management and replay detection.

The fundamental aspect of Wireless Networks in maintaining security is to preserve Confidentiality where the receiver should receive the actual transmitted information from the sender. The message authentication provides integrity to both sender as well as receiver. The Wireless Link should be always available and should be secured from outside world like malicious attacks as well as DoS Attacks (Denial of Service Attacks).

There are basically two common attacks which compromise the security and authentication mechanism of Wireless Networks i.e. Message Reply Attack and Man in the Middle Attack. The Message reply attack acts mainly on the authentication and authentication key formation protocols. The Man in the Middle Attack (MiTM) attack occurs on that security mechanism which doesn't provide mutual authentication.

Various other attacks like Session Hijacking, Reflection attacks are there which affects the security mechanism of Wireless Networks. IEEE helped in securing the wireless networks by providing the basic measures for securing wireless network and it also provide CIA factors by disabling SSID, use of MAC i.e. Media Access Control address filtering and WPA/WPS protection mechanism. The new developments in computer technology and software developments notice that these mechanisms have network vulnerable attack. So, due to these vulnerabilities WiMax standards comes into existence, for solving the short comings of 802.11 wireless networks [4]. WiMax is the new advancement in the wireless network. WiMax is still

undergoing development and still the securing problems are not being decreased by WiMax technology. It also has some drawbacks like it lack mutual authentication and is suspected to relays attacks, spoofing of MAC address of Subscriber Station (SS) and PMK authorization vulnerabilities.

IV. CONCLUSION

Wi-Fi security is not an simple task. Wireless network security is harder than wired network security. There are numerous protocols or standards or we can say technologies for wireless network security but every protocol has its demerits, until now there is no protocol which can provide security 100% or near about it. Many researchers are working on it and they are searching for the best protocol which can provide security as much as possible. WiMaX is the recent technology in the Wi-Fi security. It also has various deficiencies.

REFRENCES

[1] Wireless security: an overview by Robert J.Boncella. Washburn University ZZbonc@washburn.bdu.

[2] White paper: WLAN security Today: wireless more secure than wired by Siemens Enterprise Communications.

[3] Sara Nasre Wireless Lan Security Research Paper IT *6823* Information Security Instructor: Dr. Andy Ju An Wang Spring *2004*.

[4] Security Issues on Converged Wi-Fi & WiMAX Networks by Prof. Anand Nayyar, Lecturer, P.G. Department of Computer Science, K. L. S. D College Ludhiana ,anand_nayyar@yahoo.co.in .

[5] *Wireless network security?* Author:-Paul Asadoorian, GCIA, GCIH. Contributions by Larry Pesce, GCIA , GAWN PaulDotCom.

[6] *Securing Wi-Fi network* (10 steps of diy security) by Rakesh M Goyal and Ankur Goyal

[7] *Establishing wireless robust security networks*: a guide to IEEE 802.11i by Sheila Frankel Bernard Eydt Les Owens Karen Scarfone.

[8] *Wireless LAN security today and tomorrow* By Sangram Gayal And Dr. S. A. Vetha Manickam .

[9] *Introduction to WI-FI network security* by Bradley Mitchell, About.com.

[10] *The state of WI-FI security* by WI-FI Alliance.

[11] *WI-FI security –WEP, WPA and WPA2* by Guillaume Lehembre.

[12] *Wireless network security 802.11, Bluetooth and handheld devices* by Tom Karygiannis, Les Owens.

[13] *WEP, WPA, WPA2 and home security* by Jared Howe.